

Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2012 covering the prior calendar year 2011

1. Date filed: 02/27/2012
2. Name of company(s) covered by this certification: FTTH Communications
3. Form 499 Filer ID: 823048
4. Name of signatory: Jeffrey Feldman
5. Title of signatory: President/CEO
6. Certification:

I, Jeffrey Feldman certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

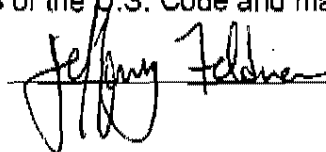
Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed



Jeffrey Feldman CEO

Attachments: Accompanying Statement explaining CPNI procedures
CPNI Compliance statements
CPNI Procedure for FTTH Communications

Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB DOCKET 06-36

The operating procedures of FTTH Communications ensures compliance with the FCC's CPNI Rules. Such procedures are as follows:

Use of CPNI in Marketing

Our company does not use CPNI in any of its marketing efforts, and does not permit the use of, or access to, customer CPNI by our affiliates or any third parties. We use, disclose or permit access to CPNI only for the purposes permitted under 47 U.S.C. Sections 222(c)(1) and (d).

Our company makes limited, one-time use of CPNI to market our communication-related services only in compliance with FCC Rule 64.2008.

We do not currently solicit for customer consent for the use of CPNI. However, before (but proximate to) soliciting customer consent for the use of CPNI to market either (a) our (or our affiliates') communication-related services; or (b) third-parties' communication-related services, we will give each customer notice of his or her right to restrict use and disclosure of, and access to, his or her CPNI, in compliance with FCC Rule 64.2008. Our company will maintain a record of these notifications for at least one year if they were to occur.

Our company does not permit access to and use of a customer's CPNI by third parties in order to market their communication-related services

Our company requires sales personnel to obtain supervisory approval of any proposed outbound marketing request for customer approval.

CPNI Safeguards

Our company has designated a compliance officer to maintain and secure the company's CPNI records and to supervise training of all company employees.

Our company trains its personnel as to when they are, and are not, authorized to use or disclose CPNI, and we have an express disciplinary process in place if the rules are violated.

Our company authenticates the identity of a customer prior to disclosing CPNI based on a customer-initiated telephone contact, online account access, or in-store visit.

Our company discloses call detail information (CDI) in a customer-initiated call only: after the customer provides a pre-established password; or, at the customer's request, by sending the CDI to the customer's address of record; or by calling back the customer at his or her telephone number of record.

Our company discloses CPNI to a customer in person at our retail location(s) only when the customer presents a valid photo ID and the ID matches the name on the account.

CPNI Recordkeeping and Reporting

Our company maintains a record of our own marketing campaigns that use customer CPNI, and do not permit any affiliates to engage in sales and marketing campaigns that use customer CPNI. We also maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. We maintain these records for at least one year.

Our company maintains records of our compliance with the FCC's CPNI Rules for use of CPNI in outbound marketing efforts, for at least one year.

Our company is prepared to provide the FCC with written notice, within five business days of any instance where the "opt out" mechanisms do not work properly.

Our company is prepared to notify the U.S. Secret Service and FBI within seven business days after the occurrence of an intentional, unauthorized (or exceeding authorization), access to, use of, or disclosure of CPNI. We may also notify the customer of such breach, after consulting with the investigatory agency(ies), if we believe there is an extraordinarily urgent need to notify a customer (or class of customers) in order to avoid immediate or irreparable harm. We will notify the customer of the breach after 7 business days following notification to the FBI and Secret Service, if such agencies have not requested that we postpone disclosure to the customer.

Our company will maintain records of any discovered breaches, notices to the Secret Service and FBI, and their responses, for at least two years.

Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB DOCKET 06-36

FTTH's Customer Proprietary Network Information (CPNI) Employee Policy and Procedures:

FTTH Employees and contractors are prohibited from releasing account information, call detail information to customers to any one, until confirmation or recognition of his/her address, Zip code or password associated with their account record has been established:

1. when a customer has initiated the call or
2. by mail or e-mail it to an address of record,
3. by calling the customer at the telephone number of record
4. or in person at FTTH's office with a valid government issued photo ID .

Account information is information that is specifically connected to the customer's service relationship with the carrier, including such things as an account number, call detail information or any component thereof, the telephone number associated with the account, or the bill's amount.

FTTH Employees shall establish a support Trouble Ticket in FTTH's secure <http://www/support.ftthcom.com> system for any CPNI breach. The Department pull down selection shall CPNI breach and the subject entered text shall be CPNI breach, with customer account information and nature of the breach entered in the information field.

In addition to the system automatically notifying the designated compliance officer (*), FTTH Employees shall notify by phone the designated compliance officer for confirmation of the CPNI breach trouble ticket.

The designated compliance officer who will then notify United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI") after discovering a breach of CPNI within 7 days of the breach. Breach records will be maintained for at least two years.

No FTTH Employee shall use CPNI information or provide CPNI information to third parties without strict supervisory approval from the designated compliance officer for any proposed outbound marketing request.

Designated Compliance Officer:

Jeffrey Feldman

Signature

